

Applic. No. 09/831,046
Response Dated August 25, 2005
Responsive to Office Action of May 27, 2005

Remarks:

Reconsideration of the present application, as amended herein, is respectfully requested.

Claims 2 - 7, 11 - 15 and 17 - 18 are now pending. Claims 7, 11, 12 and 18 have been amended. Claim 16 has been cancelled.

Applicant gratefully acknowledges that claim 16 has been indicated as being allowable if rewritten to include all the limitations of the claims from which that claim depends. More particularly, item 10 of the above-noted Office Action states, in relevant part:

Regarding claim 16, the limitations "the encoding is performed with the first key utilizing a symmetric encoding method", in combination with the elements of the parent claim have not been taught by the prior art.

Former claim 16 depended directly from claim 11. Claim 11 has now been amended to include the limitations of claim 16. Claim 16 has been canceled. As such, it is believed that claim 11 is in condition for immediate allowance. Independent claim 18 has been amended to additionally recite, among other limitations, the limitations of former claim 16 (i.e., "the encoding performed with the first key utilizing a symmetric encoding method"). As such, it is believed that claim 18 is patentable, as well.

Appl. No. 09/831,046
Response Dated August 25, 2005
Responsive to Office Action of May 27, 2005

In paragraph 3 of the Office Action, the substitute declaration was objected to as defective because the box identifying the previously-filed specification was not checked. Applicant will submit a further substitute declaration identifying the present application, prior to payment of the issue fee in the present case.

In paragraph 4 of the Office action, Claim 12 was objected to as depending from claim 1, which had been cancelled. Claim 12 has been amended herein to depend from claim 11.

In paragraph 6 of the Office Action, claim 7 was rejected under 35 U.S.C. § 112, second paragraph. More particularly, in paragraph 6 it was indicated, in relevant part:

Claim 7 recites the limitation "wherein data transmitted is confidential data" in lines 2-3. However, claim 7 depends on claim 1 in which data is also transmitted in plaintext (see clause c). It is not clear why confidential data is transmitted in plaintext which everyone, whether authorized or not, has access to.

Applicant's claim 7 currently depends from claim 11, clause c of which states:

transferring a message from the first entity to the second entity, wherein the message comprises the encoded result of the first operation as well as the uncoded result of the first operation

Applic. No. 09/831,046
Response Dated August 25, 2005
Responsive to Office Action of May 27, 2005

Clause (a) of claim 11 recites:

performing a first operation by a first entity on a prescribed known value and on a value only known to the first entity to obtain an uncoded result of the first operation;

As such, claim 7 has been amended to recite that it is the underlying prescribed known value and the value only known to the first entity that are confidential. It is believed that this is supported by the substitute specification, paragraph [0045].

It is accordingly believed that the claims meet the requirements of 35 U.S.C. § 112, second paragraph.

In item 8 of the above-identified Office Action, claims 2 - 7, 11 - 15 and 17 - 18 were rejected under 35 U.S.C. § 103(a) as allegedly being obvious over Schneier, "Applied Cryptography" ("SCHNEIER") in view of Menezes et al., "Handbook of Applied Cryptography" ("MENEZES").

Applicant believes the above rejections have been mooted by the amendment of independent claims 11 and 18 to include of the limitations of former dependent claim 16. As such, all claims now recite, among other limitations, that encoding is performed with the first key utilizing a symmetric encoding

Applic. No. 09/831,046
Response Dated August 25, 2005
Responsive to Office Action of May 27, 2005

method. Neither SCHNEIER, nor MENEZES, teach or suggest, among other limitations of Applicant's claims, the particularly claimed encoding of the result of a first operation with a first key known to a first entity and to a second entity to obtain an encoded result of the first operation, the encoding performed with the first key utilizing a symmetric encoding method.

It is accordingly believed that the cited references fail to teach or suggest, alone or in combination, the features of current independent claims 11 or 18. Claims 11 and 18 are, therefore, believed to be patentable over the art. The dependent claims are believed to be patentable as well because they all are ultimately dependent on claim 11.

In view of the foregoing, reconsideration and allowance of claims 2 - 7, 11 - 15 and 17 - 18 are solicited.

In the event the Examiner should still find any of the claims to be unpatentable, counsel would appreciate receiving a telephone call so that, if possible, patentable language can be worked out.

If an extension of time for this paper is required, petition for extension is herewith made.

Applic. No. 09/831,046
Response Dated August 25, 2005
Responsive to Office Action of May 27, 2005

Please charge any fees that might be due with respect to
Sections 1.16 and 1.17 to the Deposit Account of Lerner and
Greenberg, P.A., No. 12-1099.

Respectfully submitted,



For Applicant

Kerry P. Sisselman
Reg. No. 37,237

August 25, 2005

Lerner and Greenberg, P.A.
Post Office Box 2480
Hollywood, FL 33022-2480
Tel: (954) 925-1100
Fax: (954) 925-1101